6. Data and Asset Classification

A risk-based information data and computer asset classification scheme must be established in order to ensure that data is handled and managed appropriately. Data and computer assets must be classified in a manner that indicates the need, priorities, and expected degree of protection appropriate to the nature of the data and the potential impact of misuse.

This policy reviews the following areas:

6.1 Responsibility for Computer Assets
6.1.1 Acceptable Use of Computer Assets
6.1.2 Inventory of Computer Assets
6.1.3 Ownership of Computer Assets and Data
6.2 Information and Data Classification
6.2.1 Information and Data Classification Guidelines
6.2.2 Information and Data Classification Scheme
6.2.3 Information and Data Labeling and Handling
6.2.4 Information and Data Management
6.1 Responsibility for Computer Assets

All computer and information assets must be accounted for and have an assigned owner. Acceptable use of City assets must be understood by all employees and contingent staff.

6.1.1 Acceptable Use of Computer Assets

The acceptable use of resources, information and assets must be documented and understood by all staff (see Acceptable Use and Personnel Security Policy). Use of these resources is intended for business purposes in accordance with individual job function and responsibilities. Personal use which is limited and in accordance with the City's Ethics Ordinance, Personnel Rules and other Applicable Use policies is permitted. The limited personal use of information technology resources is not permissible if it creates a non-negligible expense to the City, consumes excessive time, or violates departmental policy. The privilege of limited personal use may be revoked or limited at any time by the City or Department officials.

a. The Information Security Office is responsible for defining acceptable use of resources, information and assets including appropriate labeling and handling procedures. In the absence of specific guidance, Information Owners and Department Management are primarily responsible to develop recommendations and minimum standards.

   HIPAA: 164.310(d)(1)(iii), ISO: 7.1.3, PCI: 12.3, 12.3.5

b. An up-to-date list of all technologies as approved/coordinated by Technical Operations and Enterprise Network Architecture must be maintained and readily available.

   PCI: 12.3.7

6.1.2 Inventory of Computer Assets

An inventory of all information assets, including systems, software, and service providers, must be kept current at all times.

a. Technical Operations and Enterprise Network Architecture must compile and maintain a data repository catalog on all third party software-related assets (e.g., application software, development tools and all third party purchased software). This catalog must be reviewed and updated annually. The catalog should contain descriptive asset information (e.g., vendor, logical locations/associated applications or systems, physical location (if applicable), owner/responsible party, information custodial responsibilities, information classification and criticality level). Business leaders are required to assist in maintaining this catalog and should communicate any changes or additions.

   HIPAA: 164.310(d)(1)(iii) ISO: 7.1.1

b. Technical Operations and Enterprise Network Architecture must compile and maintain a data repository catalog of all physical assets owned by the City. This catalog must be reviewed and updated annually. The catalog must contain descriptive asset information. Business unit managers are required to assist Technical Operations and Enterprise Network Architecture in maintaining this catalog and should communicate any changes or additions in a timely manner.

   HIPAA: 164.310(d)(1)(iii), ISO: 7.1.1, PCI 12.3.3
6.1.3 Ownership of Computer Assets and Data

Unless specifically identified and approved by the Department of Law, all information possessed or used by a particular department and all information stored and processed over the City’s technology and information systems are the property of the City and must have a designated Information Owner. City employees and contingent staff have no expectation of privacy associated with the information they store in or send through these systems, within the limits of the federal, state and local laws of the United States and, where applicable, foreign laws.

a. All physical computing assets must have an assigned Asset Owner.

b. All production information possessed or used by a particular organization or business unit within the organization must have a designated Information Owner. Ownership and custodianship of assets must be documented. HIPAA: 164.310(d)(1)(iii), ISO: 7.1.2
6.2 Information and Data Classification

Information classification is based on the level of sensitivity of the data and the potential impact of inappropriate handling should the confidentiality, integrity or availability of the information or data compromised. A classification scheme, which establishes the baseline security controls for safeguarding information, must be used to ensure appropriate security protections are placed around information during handling.

6.2.1 Information and Data Classification Guidelines

An information classification scheme must be used throughout the organization to protect City of Chicago’s assets.

a. The Information Security Office is responsible for defining the Information Data Classification scheme.

b. Information Technology Operations and Enterprise Network Architecture is responsible for management oversight of all information assets and must define procedures for proper data identification and handling.

HIPAA: 164.308(a)(7)(E), ISO: 7.2.1, PCI: 9.7.1

HIPAA: 164.308(a)(7)(E), ISO: 7.2.1, PCI: 9.7.1

HIPAA: 164.308(a)(7)(E), ISO: 7.2.1, PCI: 9.7.1

HIPAA: 164.308(a)(7)(E), ISO: 7.2.1, PCI: 9.7.1

HIPAA: 164.308(a)(7)(E), ISO: 7.2.1, PCI: 9.7.1

c. Information Owners or an assigned Information Custodian is responsible for defining the classification of an information asset.

ISO: 7.2.1

ISO: 7.2.1

ISO: 7.2.1

ISO: 7.2.1

ISO: 7.2.1

d. It is the Information Owner or delegated Information Custodian's responsibility to monitor information assets and continuously review the information's classification. The Information Owner or delegated Information Custodian must sponsor a formal declassification effort before information can be downgraded to a lower classification, based upon the definitions of the classification.

ISO: 7.2.1

ISO: 7.2.1

ISO: 7.2.1

ISO: 7.2.1

ISO: 7.2.1

e. Employees, contractors, and vendors must protect all of the City’s information in any format (e.g., hard copy, disk, tape, flash drive) at the level commensurate with its value as determined by its information classification. These standards mitigate the risk that information of different classification levels be inadvertently combined and released. Correctly classified information with proper controls can be instituted to manage the dissemination of information throughout the City’s environment.

HIPAA: 164.310(d)(1), ISO: 7.2.1

HIPAA: 164.310(d)(1), ISO: 7.2.1

HIPAA: 164.310(d)(1), ISO: 7.2.1

HIPAA: 164.310(d)(1), ISO: 7.2.1

HIPAA: 164.310(d)(1), ISO: 7.2.1
6.2.2 Information and Data Classification Scheme

The City has a four-tier classification system consisting of “Public,” “Internal”, “Sensitive” and “Confidential” levels of classification.

a. **Public** Information is defined as information that is intended for unrestricted public disclosure and is not exempt from disclosure under the Illinois Freedom of Information Act (FOIA).

   Examples include open datasets, announcements, employment advertisements, press releases and marketing materials.

b. **Internal** Information is defined as information that is related to the day to day operations of City departments and services. All internal data is subject to the Illinois Freedom of Information Act (FOIA) and if disclosed would have minimal to no impact on the confidentiality, integrity or availability of City data or computer assets.

   Examples include most business documents, minutes of meetings, emails and data related to how City services are developed and delivered.

c. **Sensitive** information is defined as information that in isolation may not present any specific risk to the confidentiality, integrity or availability of City operations, resources or constituents but if combined with other data could represent inappropriate risk. Sensitive information can be exempt from the Illinois Freedom of Information Act (FOIA). FOIA exempt information must be approved the Department of Law.

   Examples include internet protocol (IP) addresses of computer assets, design and procedure documents.

d. **Confidential** information is defined as information that if lost, disclosed, or inappropriately modified could cause significant impact to the confidentiality, integrity, availability of City operations, resources or constituents. Prior to designation, the “Confidential” classification must be approved by the Department of Law. Confidential information is exempt from disclosure under the Freedom of Information Act (FOIA).

   Examples include information related to the City’s Information Security controls, means and methods, network diagrams, passwords, data defined as Card Holder Data (CHD), Personal Health Information (PHI) and Personally Identifiable Information (PII).
6.2.3 Information and Data Labeling and Handling

All media must be labeled with its information classification to ensure the proper security controls are placed around the media while handling.

a. **Information Owners** are responsible for ensuring that all removable media containing *non-Public* data is labeled with its information classification, owner, contact information and purpose.  
   HIPAA: 164.310(d)(1), ISO: 7.2.2, PCI: 12.3.4

b. **Technology Operations and Enterprise Network Architecture** is responsible for ensuring that efforts are made to separate *Confidential* information from other information with specific security or control requirements.  
   ISO: 7.2.2

c. All employees are responsible for ensuring that any electronic information approved for deletion from computer systems and discarded hard copy documents are destroyed in a manner to protect disclosure of the information to external parties commensurate with the information's business value or confidentiality.  
   HIPAA: 164.310(d)(1)(i), ISO: 7.2.2

d. **Information Owners** or designated **Information Custodians** are responsible for ensuring that all *Confidential* information is secured in one of the following ways:
   ISO: 7.2.2
   - Hard copy information must be kept in an access-controlled room which is secured when unoccupied or within locked file cabinets with limited access if a secured room is not available; and
   - Electronic information must be encrypted using an **Information Security Office** approved method when stored on any portable device or media (e.g., laptop, hard drive, tape, compact disc, flash drive).
   HIPAA: 164.310(a)(1), ISO: 7.2.2

6.2.4 Information and Data Management

To help ensure legal and information security control of all City and constituent information, all data must remain within the United States boarders.

a. **Information Owners** are responsible to ensure that all no City owned data is forwarded to non-US locations unless as part of approved business operations which has prior approval from the **Information Security Office**.  
   NIST 800-53, FedRAMP

b. **Information Owners**, in partnership with the **Departments of Innovation and Technology**, **Procurement Services**, and **Legal** must ensure that all contracts with third-parties, who may come in contact with City data, meet or exceed NIST 800-53 and/or FedRAMP-moderate level security controls.
## Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/15/2013</td>
<td>0.5</td>
<td>Initial Draft</td>
<td>ISO</td>
</tr>
<tr>
<td>07/26/2013</td>
<td>1.0</td>
<td>Approved as Release Candidate v1</td>
<td>CISO</td>
</tr>
<tr>
<td>12/30/2013</td>
<td>2.0</td>
<td>Approved as Release Candidate v2</td>
<td>CISO</td>
</tr>
</tbody>
</table>